PENGAMANAN JARINGAN KOMPUTER MENGGUNAKAN METODE IPS (INTRUSION PREVENTION SYSTEM) TERHADAP SERANGAN BACKDOOR DAN SYNFLOOD BERBASIS SNORT INLINE

Oleh:

Mick Sandy Pratama (0834010275)

TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS PEMBANGUNAN NASIONAL

"VETERAN" JATIM

2012

Judul : Pengamanan Jaringan Komputer menggunakan Metode IPS (*Intrusion Prevention System*) terhadap Serangan *Backdoor* dan *Synflood* Berbasis Snort Inline
Pembimbing : Hudan Studiawan, S.Kom., M.Kom
Penyusun : Mick Sandy Pratama

ABSTRAK

Keamanan jaringan komputer dikategorikan dalam dua bagian keamanan fisik dan non-fisik. Keamanan fisik atau non-fisik keduanya sangat penting, namun yang terpenting adalah bagaimana cara agar jaringan komputer tersebut terhindar dari gangguan. Gangguan tersebut dapat berupa gangguan dari dalam atau luar. IPS (*Intrusion Prevention System*) adalah sebuah metode yang bekerja untuk *monitoring traffic* jaringan, mendeteksi aktivitas mencurigakan dan melakukan pencegahan dini terhadap kejadian yang dapat membuat jaringan menjadi berjalan tidak sebagaimana mestinya. Serangan yang sering dilancarkan oleh para *hacker* adalah *backdoor* dan *synflood*. *Hacker* memilih serangan *backdoor* bertujuan untuk mengakses sistem, aplikasi, atau jaringan dengan hak akses khusus, sedangkan serangan *synflood* bertujuan untuk membanjiri sistem oleh permintaan sehingga sistem menjadi terlalu sibuk dan dapat berakibat macetnya sistem (*hang*). Snort adalah sebuah *software* ringkas yang berguna untuk mengamati aktivitas dalam suatu jaringan komputer. Dari sanalah muncul penelitian-penelitian yang membahas tentang keamanan jaringan.

Banyak tool yang digunakan untuk mengamankan jaringan misalnya *firewall*, namun *firewall* saja tidak cukup efisien dalam mengamankannya. Oleh sebab itu, berkembanglah teknologi IPS dari teknologi awal IDS. Sebagai IDS, Snort hanya menganalisa paket yang ada dan memberikan peringatan bila terjadi serangan dari *hacker*. Jika seperti ini kasusnya, IDS dikatakan bekerja dalam modus pasif. Bila ingin Snort memblokir upaya serangan dan memberikan respon atas serangan *hacker* maka Snort harus berkerja sebagai IPS, Snort akan berfungsi sebagai IPS bila berjalan dalam modus *inline*.

Dari ujicoba serangan *backdoor* dan *synflood* yang telah dilakukan terbukti bahwa Snort Inline dapat melakukan drop terhadap serangan *backdoor* dan *synflood* dapat disimpulkan bahwa metode IPS lebih handal daripada Metode IDS yang hanya menganalisa packet yang ada. Sehingga disarankan untuk meningkatkan kemampuan sistem pada masa yang akan datang.

Kata Kunci: ***IPS (Intrusion Prevention System), Snort Inline, synflood, backdoor***

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa, atas semua berkat dan rahmat kasih yang dianugerahkanNya sehingga dapat terselesaikannya Tugas Akhir yang berjudul “Pengamanan Jaringan Komputer Menggunakan Metode IPS (Intrusion Prevention System) Terhadap Serangan Backdoor dan Synflood Berbasis Snort Inline”.

Penyusunan laporan tugas akhir ini diajukan untuk menyelesaikan dan memenuhi salah satu syarat yang harus ditempuh oleh setiap mahasiswa Jurusan Teknik Informatika, Fakultas Teknologi Industri Universitas Pembangunan Nasional”Veteran”Jawa Timur.

Dalam penyusunan laporan ini, penulis tidak lepas dari bantuan dan dorongan dari berbagai pihak. Oleh karena itu, pada kesempatan kali ini penulis mengucapkan terima kasih kepada :

1. Bapak Ir. Sutiyono, MT, selaku dekan FTI Universitas Pembangunan Nasional”Veteran”Jawa Timur.
2. Ibu Dr.Ir.Ni Ketut Sari, MT, selaku ketua Jurusan Teknik Informatika Universitas Pembangunan Nasional”Veteran”Jawa Timur.
3. Bapak Hudan Studiawan, S.kom , M.kom selaku dosen pembimbing , atas masukan dan bimbingannya selama ini penulis ucapkan terima kasih.
4. Bapak Kafi Ramadhani Borut, S.kom yang membantu dan membimbing saya untuk memahami Tugas Akhir ini.
5. Ibu Dr.Ir.Ni Ketut Sari, MT dan bapak Kafi Ramadhani Borut, S.kom yang telah menguji dan memberi masukan dalam Tugas Akhir ini.

6. Kedua orang tua penulis yang sepenuh hati mendukung penulis baik dalam segi materiil maupun non-materiil.
7. Adikku Vita Dian Permata Sari dan Ryan Putra Pradana yang selalu menghibur dan memberi semangat dalam penyelesaian Tugas Akhir.
8. Teman-teman angkatan 2008, yang telah banyak membantu dalam penyelesaian Tugas Akhir ini, penulis ucapkan terima kasih atas dukungan dan bantuannya.
9. Untuk seseorang yang selalu ada di hatiku Istikhomah, Amd.Keb (isty) yang selalu memberi dukungan dan motovasi dalam penyelesaian Tugas Akhir ini.
10. *My Bestfriend* (Rizal, Jefa, Agit, Darmawan, Dwiky, Abi, dan Adit) yang telah memberikan suport dan dorongan untuk menyelesaikan laporan ini.

Semoga Allah SWT memberikan balasan pahala atas segala amal baik yang telah diberikan dan semoga Tugas Akhir ini berguna bagi semua pihak yang memanfaatkan.

Surabaya, Mei 2012

Penyusun

DAFTAR ISI

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan komputer dikategorikan dalam dua bagian, yaitu keamanan secara fisik dan juga keamanan secara non-fisik. Keamanan secara fisik merupakan keamanan yang cenderung lebih memfokuskan segala sesuatunya berdasarkan sifat fisiknya. Dalam hal ini misalnya pengamanan komputer agar terhindar dari pencurian dengan rantai sehingga fisik komputer tersebut tetap pada tempatnya. Kondisi ini sudah sejak lama diaplikasikan dan dikembangkan. Sedangkan keamaanan non-fisik adalah keamanan dimana suatu kondisi keamanan yang menitikberatkan pada kepentingan secara sifat. Sebagai contoh yaitu pengamanan data, misalnya data sebuah perusahaan yang sangat penting.

Keamanan fisik ataupun keamanan non-fisik kedua–duanya sangat penting namun yang terpenting adalah bagaimana cara agar jaringan komputer tersebut terhindar dari gangguan. Gangguan tersebut dapat berupa gangguan dari dalam (internal) ataupun gangguan dari luar (eksternal). Gangguan internal merupakan gangguan yang berasal dari lingkup dalam jaringan infrastruktur tersebut. Dalam hal ini adalah gangguan dari pihak–pihak yang telah mengetahui kondisi keamanan dan kelemahan jaringan tersebut. Gangguan eksternal adalah gangguan yang memang berasal dari pihak luar yang ingin mencoba atau dengan sengaja ingin menembus keamanan yang telah ada. Gangguan eksternal biasanya lebih

sering terjadi pada jaringan eksternal, seperti web server, telnet, FTP, SSH server (Haniri, Anis, 2002).

IPS (*Intrusion Prevention System*) adalah sebuah aplikasi yang bekerja untuk monitoring *traffic* jaringan, mendeteksi aktivitas yang mencurigakan, dan melakukan pencegahan dini terhadap intrusi atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti sebagaimana mestinya. Serangan – serangan yang sering dilancarkan oleh para *hacker* antara lain *backdoor* dan *synflood*. Snort adalah sebuah *software* ringkas yang sangat berguna untuk mengamati aktivitas dalam suatu jaringan komputer.

Maka dari itu, dalam tugas akhir ini akan dirancang sebuah pengamanan jaringan komputer menggunakan metode IPS (*Intrusion Prevention System*) terhadap serangan *backdoor* dan *synflood* berbasis Snort Inline.

1.2 Rumusan Masalah

Adapun rumusan masalah yang akan dibahas dalam perancangan dan pengaplikasian keamanan jaringan komputer tersebut yaitu, pendeteksian dan pencegahan Jenis serangan - serangan hacker dalam suatu jaringan komputer khususnya jaringan eksternal antara lain :

a. Bagaimana cara mendeteksi jenis-jenis serangan yang mungkin terjadi dalam suatu jaringan komputer dengan metode IPS?
b. Bagaimana konfigurasi Snort untuk mendeteksi dan mencegah serangan *backdoor* dan *synflood (TCP-flood)*?

1.3 Batasan Masalah

Dalam perancangan dan pengaplikasian pengamanan jaringan komputer menggunakan metode “IPS *(Intrusion prevention system*)” terhadap serangan *backdoor* dan *synflood* berbasis Snort Inline ini, mempunyai batasan masalah sebagai berikut:

a. Mendeteksi serangan *backdoor* dan *synflood* dengan Snort IPS pada jaringan eksternal
b. Mencegah serangan-serangan tersebut dengan Snort yang berjalan dalam modus *inline*
c. Menggunakan VMWare sebagai simulasi jaringan komputer terdiri dari *router*, Snort Inline, dan dua *host* untuk masing-masing serangan *synflood* dan *backdoor*
d. Sarana yang diserang oleh *hacker* adalah *server* yang merupakan sistem operasi nyata dalam komputer.
e. Untuk uji coba serangan dilakukan dari jaringan internal

1.4 Tujuan Tugas Akhir

Tujuan dari tugas akhir ini adalah sebagai berikut :

a. Mengerti dan memahami jenis-jenis serangan *backdoor* dan *synflood*
b. Memahami dan mampu mengaplikasikan pendeteksian dan pencegahan serangan-serangan menggunakan metode IPS *(Intrusion Prevention System*) dengan program Snort Inline.

1.5 Manfaat Tugas Akhir

Manfaat yang didapat dari tugas akhir ini adalah sebagai berikut:

a. Meminimalisir adanya kesalahan dari sebuah sistem dalam jaringan

b. Mengamankan sebuah jaringan komputer yang berbasis *client-server*

c. Mengamankan jaringan lokal maupun jaringan internet

1.6 Sistematika Penulisan

Sistematika penulisan Tugas Akhir (TA) ini akan membantu mengarahkan penulisan laporan agar tidak menyimpang dari batasan masalah yang dijadikan sebagai acuan atau kerangka penulisan dalam mencapai tujuan penulisan laporan Tugas Akhir (TA) sesuai dengan apa yang diharapkan. Laporan Tugas Akhir (TA) ini terbagi dalam empat bab yaitu:

BAB I: PENDAHULUAN

Pendahuluan berisi mengenai gambaran umum tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan, manfaat dan sistematika penulisan.

BAB II: TINJAUAN PUSTAKA

Tinjauan pustaka ini berisi tentang gambaran umum objek pekerjaan, pengertian–pengertian dasar dan teori–teori yang berhubungan dengan masalah yang akan dibahas dalam tugas akhir (TA) ini sebagai landasan bagi pemecahan yang diusulkan.

BAB III: METODE TUGAS AKHIR

Metode tugas akhir ini berisi tentang rancangan jaringan, rancangan pendeteksian serangan-serangan, dan metode-metode yang dipakai untuk penyelesaian tugas akhir.

BAB IV: IMPLEMENTASI SISTEM

Implementasi sistem berisi tentang hasil dan pembahasan mengenai

beberapa konfigurasi-konfigurasi untuk membentuk sebuah keamanan untuk jaringan komputer serta timbal balik pengamanan dari serangan *backdoor* dan *synflood*.

BAB V: KESIMPULAN DAN SARAN

Berisi tentang kesimpulan yang di peroleh dari hasil pengana-lisaan data dari bab-bab sebelumnya. Selain itu bab ini berisi tentang saran-saran yang diharapkan dapat bermanfaat dan dapat membangun serta mengembangkan isi laporan terebut sesuai dengan tujuan penulisan Laporan Tugas Akhir (TA).

BAB VI: PENUTUP

Berisi daftar pustaka dan lampiran-lampiran lain yang berfungsi untuk melengkapi uraian yang disajikan dalam bagian utama laporan.